UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

MARY SHELOR, individually and on behalf of all others similarly situated, Plaintiff, v. CHANGE HEALTHCARE INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Mary Shelor ("Plaintiff"), on behalf of herself and all others similarly situated, brings this Class Action Complaint against Defendant Change Healthcare Inc. ("Defendant"). Plaintiff alleges upon knowledge to herself and upon information and belief as to all other matters as follows.

INTRODUCTION

1. Plaintiff brings this class action as a result of Defendant's failure to properly secure and safeguard highly sensitive personal information which was accessed and/or exfiltrated by unauthorized third parties during a data breach that exploited a vulnerability in its software technology on or about February 21, 2024 (the "Data Breach").

2. The information compromised in the Data Breach includes both personally identifiable information ("PII") and protected health information ("PHI"), such as, patient medical and patient payment information.[1]

[1] *Update: Some Applications are Experiencing Connectivity Issues., Incident Report for Optum Solutions*, Optum, https://status.changehealthcare.com/incidents/hqpjz25fn3n7 (last accessed Mar. 22, 2024).

3. As a sophisticated and leading provider of health information technology services Defendant is or should have been aware, this type of personal and sensitive data is highly targeted and sought after by hackers who seek to exploit that data for nefarious purposes. In the wrong hands, these types of sensitive data allow criminals to cause significant harm to individuals including Plaintiff and the Class Members.

4. Defendant Change Healthcare Inc. is a health technology company that provides pharmacies and health care providers in the United States with tools that allow them to electronically process claims and other essential payment and revenue management practices.[2] As part of its business operations, Change Healthcare provides software applications and tools to its client.

5. Change Healthcare's software is used by many healthcare providers including *inter alia* pharmacies, medical offices/practices and other medical providers to allow technicians the ability to deliver services through direct remote access to desktops, mobile devices, and more.

6. Since the Data Breach on or about February 21, 2024, a multitude of pharmacies and healthcare providers have announced that their data was part of and exfiltrated in the Data Breach, and therefore the data of millions of their customers, clients, and/or members, has also been impacted. The large number of companies that have reported being impacted by the breach underscores the widespread effect and deep consequences of this Data Breach.[3]

7. The ransomware group known as "ALPHV/BlackCat" claim responsibility for the cyberattack facilitated by exploiting the vulnerability in Change Healthcare's software in order to

[2] Change Healthcare, https://www.changehealthcare.com/platform (last accessed Mar. 22, 2024).
[3] *See, e.g.*, *Pharmacies Across US Disrupted Following Hack at Change Healthcare Network,* Reuters (Feb. 22, 2024), https://www.reuters.com/business/healthcare-pharmaceuticals/change-healthcare-network-hit-by-cybersecurity-attack-2024-02-22/ (last accessed Mar. 22, 2024).

exfiltrate data from the underlying databases.[4] It claims to have accessed Change Healthcare servers and seized 6 terabytes of crucial confidential and highly sensitive information resulting in network outages that have already impacted millions of patients, pharmacies and physicians across the country.

8. Blackcat is a notable cybergroup that infiltrates healthcare institutions' internal servers through vulnerabilities in their networks. The group uses "ransomware to dentify and attack 'high-value victim institutions[.]'"[5] CISA reports that ALPHV/BlackCat has been known both to exfiltrate data and to ransom exfiltrated data for profit.[6]

9. According to the Department of Justice, Blackcat typically steals victims' data and encrypts the institution's data, networks, and servers, blocking the institution from accessing them. The group then demands the institution pay a ransom in exchange for the keys to decrypt the institution's network and servers. In exchange for ransom, Blackcat also offers a promise that it will not publish the institution's data to Blackcat's site on the Dark Web. Still, even when ransoms are paid, this data often ends up on the Dark Web. Blackcat has emerged as the second most prolific ransomware-as-a-service variant in the world.[7]

10. According to The HIPAA Journal, "The Blackcat ransomware ground claims to have stolen a vast amount of data from Change Healthcare in the recent cyberattack. In a statement

---

[4] *ALPHV/BlackCat Responsible For Change Healthcare Cyberattack*, The Register (Feb. 26, 2024), https://www.theregister.com/2024/02/26/alphv_healthcare_unitedhealth/ (last accessed Mar. 22, 2024).
[5] James Farrell, *Change Healthcare Blames 'Blackcat' Group for Cyber Attack That Disrupted Pharmacies and Health Systems*, FORBES (Feb. 29, 2024, 1:18 PM), https://www.forbes.com/sites/jamesfarrell/2024/02/29/change-healthcare-blames-blackcat-groupfor-cyber-attack-that-disrupted-pharmacies-and-health-systems/?sh=589769fc1c4d.
[6] *#StopRansomeware: ALPHV Blackcat*, Cybersecurity and & Infrastructure Sec. Agency (updated Feb. 27, 2024) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a (last accessed Mar. 22, 2024).
[7] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcatransomware-variant.

posted, and later removed, from its data leak site, a member of the group claimed to have stolen 6TB of data from UnitedHealth, which the group alleges includes "highly selective data" from all Change Healthcare clients, including Medicare, CVS Caremark, Health Net, and Tricare, the U.S. military medical health agency. Screenshots of some of the data were shared as proof of data theft. The group also claims to have stolen the source code of Change Healthcare applications. The group claims to have stolen the data of millions of patients, including medical records, insurance records, dental records, payment information, claims information, and patients' PHI, including health data, contact information, and Social Security numbers."[8]

11. Change Healthcare has confirmed that ALPHV/BlackCat was behind the cyberattack. Specifically, Change Healthcare issued a statement confirming that it is "experiencing a cybersecurity issue perpetrated by a cybercrime threat actor who has represented itself to us as ALPHV/Blackcat."[9] The Company's notice to customers further stated. "Our experts are working to address the matter and we are working closely with law enforcement and leading third-party consultants, Mandiant and Palo Alto Network, on this attack against Change Healthcare's system. We are actively working to understand the impact to members, patients and customers."[10]

12. While Change Health is attempting to figure things out, this Data Breach is wreaking havoc on the healthcare industry and negatively impacting health care providers,

[8] The HIPAA Journal (Feb. 29, 2024), https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/ (last accessed Mar. 22, 2024)
[9] *Change Healthcare Cyberattack Fallout Continues*, Tech Target (Feb. 29. 2024), https://healthitsecurity.com/news/change-healthcare-disconnects-system-amid-cyberattack#:~:text=Change%20Healthcare%20has%20confirmed%20that,latest%20notice%20to%20customers%20stated. (last accessed Mar. 22, 2024).
[10] *Id.*

patients and consumers. Change Health as part the largest healthcare insurer, processes 15 billion transactions annually, "touching one in three U.S. patient records."[11]

13. Change Health responded to the Data Breach to stop the cybersecurity wound by taking certain systems offline. With Change Health and its related entities systems offline and not operating, the healthcare industry is immobilized and shut down. Patients are not able to get their prescriptions filled and take crucial and vital medications to treat their health conditions. This is especially disruptive to elderly patients who have a fixed income and cannot afford medications without insurance, as well as individuals with chronic illnesses who face life-threatening symptoms without their medication. Change Health and its related entities shutting down its systems and network outage is jeopardizing not only the health of millions of Americans, but also impacted the ability for healthcare providers to provide medical care and services to patients.

14. Patients are not the only victims here. The cascading effect of the Data Breach is also impacting and drastically affecting healthcare providers' practices. [T]his cyberattack has affected every hospital in the country one way or another."[12] Many medical providers are having difficulty verifying patient eligibility and insurance coverage, filing claims for reimbursement and billing patients.[13] As a result these providers are not able to get paid which

[11] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-accessstill-impacted/.
[12] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-accessstill-impacted/.
[13] Associated Press, *Minnetonka Based United Healthcare Hacked*, KNSI (Feb. 29, 2024, 5:46 PM), https://knsiradio.com/2024/02/29/minnetonka-based-united-healthcare-hacked/.

negatively impacts their ability to run and operate their business. Without being able to be paid or reimbursed from insurers for patient treatment and care medical providers have had to cut payroll, medical supplies and other services and care.

15. The Data Breach was a direct and proximate result of Defendant's failure to implement and follow reasonable security procedures and practices and failed to disclose material facts surrounding its deficient security protocols, procedures and practices. As a result of Defendant's negligence, patients and healthcare providers will be impacted and feel the effects that the shutdown and network outage for weeks. And Plaintiff's and Class Members' whose PII and PHI was stolen and is now in the hands of criminals will feel the impact for the rest of their respective lives. Plaintiff and Class Members now face a substantially increased risk of identity theft, both currently and for the indefinite future, at least in part because their PII and PHI is now being offered and sold to identity thieves to engage in scams and other harms caused by the disclosure of their PII and PHI. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to Defendant's actions.

16. As a result of Defendant's failure to protect the confidential and sensitive information it was entrusted to safeguard , Plaintiff and Class members did not receive the benefit of their bargain with Defendant and now face a significant risk of medical related theft and fraud, financial fraud, and other identity-related fraud now and into the indefinite future.

17. Plaintiff brings this Complaint on behalf of herself and all persons whose PII and/or PHI was stolen during the Data Breach. Plaintiff asserts claims for negligence, negligence per se, and declaratory judgment.

PARTIES

18. Plaintiff Mary Shelor is a citizen and resident of the Commonwealth of Pennsylvania who fills her prescription at a local CVS pharmacy that uses Change Healthcare 's platform and systems.

19. Defendant Change Healthcare Inc. is a for-profit Delaware corporation with its principal place of business located at 424 Church Street, Suite 1400, Nashville, Tennessee 37219. Defendant Change Healthcare is a citizen of the States of Delaware and Tennessee.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this proposed class action pursuant to 28 U.S.C. § 1332(d), under the provisions of the Class Action Fairness Act, which specifies that the federal courts maintain original jurisdiction in any class action in which at least 100 members are in the proposed plaintiff class, any member of the plaintiff class is a citizen of a state different from any defendant, and the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs. Plaintiff submits that all such conditions are satisfied such that this Court has original jurisdiction.

21. This Court has specific personal jurisdiction over Defendant Change Healthcare because it is a citizen of this District, registered to conduct business in this District, maintains its principle place of business in this District, has continuous and systematic contacts with this District, does substantial business in and within this District, receives substantial revenues from marketing, distribution, and sales in this District, so as to subject itself to the personal jurisdiction of this District, and thus rendering the exercise of jurisdiction by this Court proper and necessary.

22. This Court is the proper venue for this case pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to Plaintiff's claims occurred in Tennessee and because Defendant conducts a substantial part of its business within this District.

FACTUAL ALLEGATIONS

A. Defendant Provides Technology Services Involving Highly Sensitive Data.

23. Defendant Change Healthcare is a Tennessee-based healthcare services and support company that provides remote access software to pharmacies and healthcare providers to communicate with patients and facilitate the electronic adjudication of claims and payments.[14]

24. In order to provide these services, Change Healthcare acquires, collects, and stores the PII and PHI of the individual-patients with whom its pharmacies and healthcare providers service, including those individuals' names, contact details, healthcare insurance information, medical records, dental records, and payment information.

25. Due to the sensitivity of the PII and PHI that Change Healthcare handles, it is aware of its duty and responsibility to safeguard and protect this information.

26. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and PHI, Change Healthcare assumed equitable and legal duties to safeguard, protect and keep confidential Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures. Change Healthcare acknowledges its understanding of these duties by promising that "Change Healthcare is committed to the privacy and security of healthcare data and meets or exceeds HIPAA Privacy and Security Rule requirements."[15]

27. However, despite undertaking and acknowledging these duties, Change Healthcare failed to implement reasonable data security measures to protect and safeguard Plaintiff's and

[14] Change Healthcare, *supra* note 2.
[15] *Privacy And Security*, Change Healthcare, https://support.changehealthcare.com/customer-resources/hipaa-simplified/privacy-security (last accessed Mar. 22, 2024).

Class Members' PII and PHI. Its failure to do so resulted in third-party hackers accessing and compromising Plaintiff's and Class Members' PII and PHI as part of the Data Breach.

28. Upon information and belief, Change Healthcare utilizes remote access software and on-premises hardware to conduct its business operations. By using on-premises hardware, *i.e.*, a server, Change healthcare had physical control over the server that was compromised at the time of the Data Breach.

29. Despite Defendant's promise to protect sensitive data and efforts to portray themselves as capable data custodians, Defendant's own data security decisions created substantial gaps that Defendant knew or should have known created a risk of a data breach. That risk materialized in February 2024, when hackers broke into Defendant's system and stole highly sensitive data and put Plaintiff and Class Members at risk that their data would be misused and cause them harm for their respective lifetimes.

B. Change Healthcare is Subject to HIPAA as a Business Associate of Covered Entities.

30. Change Healthcare is a HIPAA covered business associate that provides services to various healthcare providers (*i.e.*, HIPAA "Covered Entities"). As a regular and necessary part of its business, Change Healthcare collects and stores the highly sensitive PHI of its clients' patients. Change Healthcare is required under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects, and Change Healthcare is further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

31. Change Healthcare is obligated to implement reasonable data security measures to protect persons' PII and PHI. As a HIPAA covered business associate, Change Healthcare is required to enter into contracts with its Covered Entities to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of PHI, including by implementing

requirements of the HIPAA Security Rule and to report to the Covered Entities any unauthorized use or disclosure of PHI, including incidents that constitute breaches of unsecured PHI as in the case of a data breach like the one complained of herein.

32. As a condition of receiving Change Healthcare's services, Change Healthcare requires that Covered Entities and their patients, including Plaintiff and Class Members, entrust it with highly sensitive personal information. Due to the nature of Change Healthcare's business, which includes providing remote access software to pharmacies and healthcare providers, Change Healthcare would be unable to engage in its regular business activities without collecting and aggregating PHI that it knows and understands to be sensitive and confidential.

33. Plaintiff's and Class Members' PII and PHI was maintained and/or received by Change Healthcare through its pharmacies and healthcare provider clients. As such Change Healthcare was entrusted to implement reasonable data security measures to protect such information.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' sensitive information, Change Healthcare assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII and/or PHI from unauthorized disclosure.

35. Further, given the application of HIPAA to Change Healthcare, and that Plaintiff and Class Members directly or indirectly entrusted their PHI to Change Healthcare in order to receive healthcare services, Plaintiff and Class Members reasonably expected that Change Healthcare would safeguard their highly sensitive information and keep their PHI confidential.

C. Defendant Failed to Safeguard Plaintiff's and Class Members' Information and Exposed PII and PHI to Hackers.

36. Upon information and belief, Change Healthcare provides remote network software and services to its clients.

37. Upon information and belief, Change Healthcare provides software allowing its clients to navigate their health networks remotely.

38. Beginning on or around February 21, 2024, the notorious ALPHV/BlackCat ransomware gang exploited a vulnerability in Defendant's software and accessed, copied, and stole Plaintiff's and Class Members' PII and PHI that was processed and stored on Change Healthcare's server.[16]

39. According to information posted by a member of the ALPHV/BlackCat group who claimed to have stolen 6TB of data from UnitedHealth, which the group alleges includes "highly selective data" from all Change Healthcare clients, including Medicare, CVS Caremark, Health Net, and Tricare, the U.S. military medical health agency. Screenshots of some of the data were shared as proof of data theft. The group also claims to have stolen the source code of Change Healthcare applications. The group claims to have stolen the data of millions of patients, including medical records, insurance records, dental records, payment information, claims information, and patients' PHI, including health data, contact information, and Social Security numbers.[17]

40. The vulnerability allowed ALPHV/BlackCat to bypass authentication restrictions and gain unauthorized access to customer environments.[18]

41. On February 22, 2024, United Health Group Incorporated filed a Form 8-K confirming that on February 21, 2024, it identified a suspected nation-state associated cyber

[16] CISA, *supra* note 6.
[17] The HIPAA Journal, *supra* note 8.
[18] CISA, *supra* note 6.

security threat actor had gained access to some of the Change Healthcare information technology system.[19]

42. Based on Change Healthcare's reporting, the information compromised in the Data Breach includes, *inter alia*, patient medical records, patient dental records, and patient payment information.

43. Despite the Data Breach occurring on or about February 21, 2024, Change Healthcare has not formally notified impacted patients of the Data Breach.

44. Upon information and belief, the Data Breach occurred as a direct result of Defendant's failure to implement and follow reasonable data security procedures in order to protect individuals' PII and PHI.

D. Defendant's Insufficient Data Security Caused the Data Breach.

45. Security experts, both private and governmental, have long warned companies that data security must be a top priority. The Federal Trade Commission ("FTC"), for example, has also issued numerous guidelines for businesses highlighting the importance of reasonable data security practices. The FTC notes the need to factor data security into all business decision-making.[20] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; using industry tested and accepted security methods; (5) monitoring activity on networks to uncover unapproved activity; (6) verifying that privacy and security features function

[19] *See* UnitedHealth Group Inc., Current Report (Form 8-K), SECURITIES AND EXCHANGE COMMISSION (Feb. 22, 2024), https://www.sec.gov/Archives/edgar/data/731766/000073176624000045/unh-20240221.htm (last accessed Mar. 22, 2024).

[20] *Start with Security A Guide For Business, Lessons Learned from FTC Cases*, Federal Trade Comm'n (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Mar. 22, 2024).

properly; (7) testing for common vulnerabilities; and (8) updating and patching third-party software.[21]

46. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act").

47. As such, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ⁋ 7 (June 15, 2011) ("[Defendants] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ⁋ 7 (Mar. 7, 2006) ("[Defendants] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendants] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which

[21] *Id.*; Federal Trade Comm'n, *Protecting Personal Information, A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Mar. 22, 2024).

all proceeded Defendant's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

48. Although Defendant's business involves handling highly sensitive data, Defendant failed to implement adequate data security practices and by doing so knew or should have known, especially as a technology company and purported expert in the field, it put its clients and its client's customers at risk of having their PII and PHI exposed.

E. The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

49. It is well known that PHI and PII are highly sensitive and are frequent, intentional targets of cybercriminals. Companies that collect and handle such information, including Defendant, are well aware of the risk of being targeted by cybercriminals.

50. Defendant also knew that a breach of its computer system, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

51. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred such as Progress Software, Fortra, T-Mobile, Equifax, Facebook, Yahoo, Marriott, Anthem, and others.

52. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been a "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[22] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

[22] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last accessed Mar. 22, 2024).

53. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the IRTC, in 2022, there were 1,802 reported data compromises in the United States, the second highest number of data events in a single year and only 60 events short of the record high number of events that occurred in 2021.[23] Of the 1,802 compromises reported in 2022, 98.4% were data breaches, affecting at least 392,180,551 victims in total, and 83% involved the exposure of sensitive records.[24]

54. In tandem with the increase in data breaches, the rate of identity theft and the resulting losses has also increased over the past few years. The Bureau of Justice Statistics reported that, in 2021, about 23.9 million people in the United States were victims of an identity theft incident, and their losses totaled $16.4 billion.[25] The increasing rate of identity theft is apparent from the directly preceding Bureau of Justice publication, which covered the data from 2018. From 2018 to 2021, the number of persons affected increased by approximately one million, and monetary losses increased by $1.3 billion.[26]

55. PII has considerable value and constitutes an enticing and well-known target for cybercriminals. Hackers can easily sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[27] PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

---

[23] *Data Breach Reports: 2022 End of Year Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 25, 2023), at 7, https://www.idtheftcenter.org/publication/2022-data-breach-report (last accessed Mar. 22, 2024).
[24] *Id.* at 6, 21.
[25] Erika Harrell & Alexandra Thompson, Victims of Identity Theft, 2021, BUREAU OF JUST. STAT. (Oct. 2023, NCJ 306474), https://bjs.ojp.gov/document/vit21.pdf (last accessed Mar. 22, 2024).
[26] Erika Harrell, Victims of Identity Theft, 2018, BUREAU OF JUST. STAT. (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed Mar. 22, 2024).
[27] Krebs, *supra*, note 22.

56. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020 [28]

57. Because of the value of PHI, the healthcare industry, specifically, has become a prime target for threat actors: "High demand for patient information and often-outdated systems are among the nine reasons healthcare is now the biggest target for online attacks."[29] Indeed, "[t]he IT environments of healthcare organizations are often complex and difficult to secure. Devices and software continue to be used that have reached end-of-life, as upgrading is costly and often problematic. Many healthcare providers use software solutions that have been developed to work on specific – and now obsolete – operating systems and cannot be transferred to supported operating systems."[30]

58. Additionally, "[h]ospitals store an incredible amount of patient data. Confidential data that's worth a lot of money to hackers who can sell it on easily – making the industry a growing target."[31]

59. Cybercriminals seek out PHI at a greater rate than other sources of personal information. Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more individuals

[28] *2022 Breach Barometer*, Protenus, https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer (last accessed Mar. 22, 2024).
[29] *The Healthcare Industry is at Risk*, SwivelSecure https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/ (last accessed Mar. 22, 2024).
[30] Steve Alder, Editorial: *Why Do Criminals Target Medical Records*, HIPAA Journal (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records/#:~:text=Healthcare%20records%20are%20so%20valuable,credit%20cards%20in%20victims'%20names (last accessed Mar. 22, 2024).
[31] *Id.*

have been reported to Health and Human Services' Office of Civil Rights, resulting in the exposure or unauthorized disclosure of the information of 382,262,109 individuals— "[t]hat equates to more than 1.2x the population of the United States."[32]

60. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[33]

61. In light of recent high profile data breaches at other health care partner and provider companies, Defendant knew or should have known that its electronic records and consumers' PII and/or PHI would be targeted by cybercriminals and ransomware attack groups.

62. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves the patients of the healthcare providers using Change Healthcare's services especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

63. As indicated by Jim Trainor, former second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[34] A complete identity theft kit that includes health insurance credentials may be

---

[32] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last accessed Mar. 22, 2024).

[33] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), https://healthitsecurity.com/news/health-sector-suffered-337-healthcare-data-breaches-in-first-half-of-year (last accessed Mar. 22, 2024).

[34] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last accessed Mar. 22, 2024).

worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.[35]

64. According to Experian:

> Having your records stolen in a healthcare data breach can be a prescription for financial disaster. If scam artists break into healthcare networks and grab your medical information, they can impersonate you to get medical services, use your data open credit accounts, break into your bank accounts, obtain drugs illegally, and even blackmail you with sensitive personal details.
>
> ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that healthcare identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills.
>
> Victims of healthcare data breaches may also find themselves being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores. In the worst cases, they've been threatened with losing custody of their children, been charged with drug trafficking, found it hard to get hired for a job, or even been fired by their employers.[36]

65. Further, according to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have [sic] been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[37]

---

[35] *Managing Cyber Risks in an Interconnected World, Key Findings from the Global State of Information Security® Survey 2015*, PriceWaterhouseCoopers, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last accessed Mar. 22, 2024).

[36] Brian O'Connor, *Healthcare Data Breach: What to Know About them and What to Do After One*, Experian (June 14, 2018), https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed Mar. 22, 2024).

[37] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Mar. 22, 2024).

66. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII and PHI about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

67. Based on the value of its patients' PII and PHI to cybercriminals, Defendant certainly knew the importance of safeguarding that information as well as the foreseeable risk of failing to do so. However, Defendant still failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Defendant Failed to Comply with FTC Guidelines.

68. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.[38]

69. The FTC's publication, "*Start with Security: A Guide for Business*," sets forth cybersecurity guidelines and best practices for businesses.[39] These guidelines note, *inter alia*, that businesses should: (a) protect the personal customer information they collect and store; (b)

[38] *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).
[39] Fed. Trade Comm'n, *supra*, note 21.

properly dispose of personal information that is no longer needed; (c) encrypt information stored on computer networks; (d) understand network vulnerabilities; (e) implement policies to correct security problems. The FTC guidelines further recommend that all businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[40]

70. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Defendant was at all times fully aware of its obligation to protect the PII and PHI of patients because of its position as a business associate, which gave it direct access to reams of patient PII and PHI from the healthcare providers with which it contracts. Defendant was also aware of the significant repercussions that would result from its failure to do so.

72. Despite its obligation, Defendant failed to properly implement basic data security practices, and Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

G. Defendant Failed to Comply with HIPAA Guidelines.

73. As Change Healthcare is a HIPAA covered business associate, it must comply with the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

[40] *Id.*

74. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes standards for the protection of health information.

75. Similarly, HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a set of security standards for protecting health information that is kept or transferred in electronic form.

76. As a covered business associated, Defendant was required to "comply with the applicable standards, implementation specifications, and requirements of" HIPAA as it pertains to "electronic protected health information." 45 CFR § 164.302.

77. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

78. HIPAA's Security Rule requires entities like Change Healthcare to, *inter alia*, ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and, ensure compliance by its workforce.

79. HIPAA further requires entities like Change Healthcare to ""review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.306(e), 45 C.F.R. § 164.312(a)(1).

80. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and (a)(3); *see also* 32 U.S.C. § 17902.

81. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

H. Defendant Failed to Comply with Industry Standards.

82. As discussed herein, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the PII and/or PHI which they collect and maintain.

83. Several best practices have been identified that at a minimum should be implemented by healthcare services like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

84. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

85. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5,

PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

86. Moreover, Defendant failed to institute common sense security measures such as network segmentation and POLP, which itself is known as a "cybersecurity best practice.[41] Had they been in place, at best the Data Breach could have been prevented all together, or at worst the scope of the Data Breach would have been severely limited.

87. Upon information and belief, Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

I. Plaintiff's Experience.

88. Plaintiff Mary Shelor uses CVS Pharmacy to fill her medical prescriptions.

89. For purposes of receiving medical treatment, Ms. Shelor was required to provide her healthcare provider with her sensitive personal information, including, among other information, her full name, contact information, date of birth, Social Security number, and health insurance information.

90. Ms. Shelor's healthcare provider also maintained her patient account numbers, health insurance information, medical record numbers, dates of service, provider names, and medical and clinical treatment information.

91. Ms. Shelor's healthcare provider shared her PHI with CVS Pharmacy in connection with filling Ms. Shelor's prescription. CVS stored Ms. Shelor's PHI in its systems and then shared

[41] "DEFINITION principle of least privilege (POLP)" https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP (last accessed Mar. 25, 2024).

it with Defendant in connection with filling her prescriptions. Defendant stored Ms. Shelor's PHI in its system.

92. Ms. Shelor learned of the Data Breach after having challenges filling her prescription. On or about March 6, 2024, she went to fill her prescription at her local CVS Pharmacy but was unable to do so.

93. Ms. Shelor uses a discount card provided by the drug manufacturer to defray the cost of her medication. On or about March 6, 2024, Ms. Shelor was notified by CVS personnel that they could not verify the validity of her discount card in their records.

94. At recent visits, CVS had been able to verify her card from their records. CVS was able to offer no reason for this loss of her records. Upon information and belief, the record of Ms. Shelor's card at CVS was lost due to the recent cyberattack.

95. Because CVS had no record of Ms. Shelor's discount card, she was told she would have to pay $957.00 to receive her medication that day. $957.00 was a significantly higher price than she was accustomed to paying.

96. Ms. Shelor was unable to pay $957.00 for her medication and was unable to timely fill her prescription subjecting her to potential negative health risks.

97. Since she could not afford the cost of her medication, Ms. Shelor had to wait twelve (12) days to fill her prescription. During those twelve (12) days she did not take her medication and missed at least one (1) day of work due to her untreated medical condition. She was also required to re-register with the drug manufacturer for the discount card.

98. Because the Data Breach impacted PHI of patients associated with CVS Pharmacy, Ms. Shelor has spent time and effort researching the breach and reviewing her financial and medical account statements for evidence of unauthorized activity, which she will continue to do

indefinitely. In addition to the ramifications associated with not being able to timely access necessary medications, Ms. Shelor also suffered emotional distress knowing that her highly personal medical and treatment information is no longer confidential and can be used for blackmail, extortion, medical related identity theft or fraud, and any number of additional harms against her for the rest of her life.

99. Since the announcement that PII and PHI was exposed to unknown third parties as a result of the Data Breach, Ms. Shelor has spent her valuable time monitoring her various accounts in an effort to detect and prevent any misuses of her PII and PHI – time which she would not have had to expend but for the Data Breach. Additionally, she has spent time in response to the Data Breach, investigating and researching the Data Breach and determining what sensitive PHI and PII has been exposed and is now available for sale.

100. Given the nature of the information the hackers claim to have exfiltrated in the Data Breach, including medical records, insurance records, dental records, payment information, claims information, and patients' PHI, including health data, contact information, and Social Security numbers, and the propensity of cybercriminals to use such information to commit a wide variety of financial and medical identity theft and fraud crimes, Plaintiff has been and will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come. Such a risk is certainly impending and is not speculative, given that information from the Data Breach is on the dark web and already being offered for sale.

J. Defendant Change Healthcare Data Breach Response is Inadequate.

101. Upon information and belief, the Data Breach affected millions of individuals across the United States.

102. Despite the breadth of the Data Breach's effects, Change Healthcare's response lacked sufficient information and remedies.

103. For one, Change Healthcare stated that it learned that patients' PII and PHI were on its breached server on February 21, 2024, yet has still failed to provide formal notice to those impacted by the Data Breach.

K. Plaintiff and Class Members Suffered Damages Due to the Data Breach.

104. Cyberattacks and data breaches at companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

105. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[42]

106. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[43]

107. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[44]

108. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

---

42 *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Mar. 22, 2024).

43 *See* Sung J. Choi et al., Data Breach Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Mar. 22, 2024).

44 *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Mar. 22, 2024).

109. Moreover, theft of Private Information is also gravely serious. Private Information is an extremely valuable property right.[45]

110. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

111. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways.

112. Plaintiff and Class Members entrusted their PII and PHI to Defendant's clients in order to receive healthcare services. Their information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

113. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having their identities stolen, their medical information used for improper purposes, medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

114. Further, as a direct and proximate result of Defendant's actions and omissions, Plaintiff and Class Members have been forced to deal with the effects of the Data Breach.

45 *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

115. Plaintiff and Class Members must immediately devote time, energy, and money to mitigating the effects of the Data Breach. These mitigation measures include:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

116. Moreover, Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their personal data, since potential fraudsters will likely use such information to carry out such targeted schemes against Plaintiff and Class Members.

117. The PII and PHI maintained by and stolen from Defendant's system, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff

and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

118. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their personal, PII and/or PHI—which contains the most intimate details about a person's life, including details of physical and mental ailments, financial standing, and other sensitive information—may be disclosed to the entire world, thereby stripping away their privacy and potentially subjecting them to embarrassment.

119. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

120. Plaintiff brings this action against Defendant on behalf of herself and all other persons similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

121. Specifically, Plaintiff seeks to represent a Class defined as follows:

> All individuals in the United States and its territories whose PII and/or PHI were compromised in the Change Healthcare Data Breach that occurred on or around February 21, 2024 (the "Class").

122. Excluded from the Class are Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

123. The proposed Class is defined based on the information available to Plaintiff at this time. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

124. Numerosity. The proposed Class is so numerous that joinder of all members is impracticable. The size of the putative class is believed to be in excess of eight million individuals. In addition, the names of all potential members of the proposed Class are not known.

125. Commonality. The questions of law and fact common to the proposed Class predominate over any questions affecting only individual members. These questions of law and fact include, but are not limited to:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII and/or PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant was negligent in maintaining, protecting, and securing PII and/or PHI;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

e. Whether Defendant's response to the Breach was reasonable;

f. Whether the Data Breach caused Plaintiff's and the Class's injuries;

g. What the proper damages measure is; and

h. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

126. Typicality. The claims of Plaintiff are typical of the claims of the proposed Class. Plaintiff and putative class members were all victims due to Defendant's policies and willful practices of failing to reasonably safeguard their PII and PHI leading to it being obtained by an unauthorized third party.

127. Adequacy of Representation. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of Class Members. Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to those of the other Members of the Class, and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. In addition, Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

128. Superiority. This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all Class Members is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

129. Predominance. Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages are common to Plaintiff and each member of the Class. If Defendant

breached its duty to Plaintiff and Class Members, then Plaintiff and each Class Member suffered damages by that conduct.

130. Injunctive Relief. Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

131. Ascertainability**:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

132. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs.

133. Defendant owed a duty to Plaintiff and the members of the Class to take reasonable care in managing and protecting the highly sensitive data it managed and stored on behalf of its clients. This duty arises from multiple sources.

134. Defendant owed a common law duty to Plaintiff and Class Members to implement reasonable data security measures because it was foreseeable that hackers would target Defendant's data system, software, and servers containing Plaintiff's and the Class's sensitive data and that, should a breach occur, Plaintiff and Class Members would be harmed. Defendant alone controlled its technology, infrastructure, and cybersecurity. Defendant further knew or should have known that if hackers breached its data system, they would extract sensitive data and inflict injury upon Plaintiff and Class Members. Furthermore, Defendant knew or should have known that if hackers accessed the sensitive data, the responsibility for remediating and mitigating the consequences of the breach would largely fall on individual persons whose data was impacted and

stolen. Therefore, the Data Breach, and the harm it caused Plaintiff and Class Members, was the foreseeable consequence of Defendant's unsecure, unreasonable data security measures.

135. Change Healthcare is a HIPAA covered business associate that provides services to various healthcare providers (*i.e.*, HIPAA "Covered Entities"). As a regular and necessary part of its business, Change Healthcare was required to implement reasonable data security measures because it collects and stores the highly sensitive PHI of its clients' patients. Change Healthcare is required under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects, and Change Healthcare is further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

136. Additionally, Section 5 of the FTC Act, 15 U.S.C. § 45, required Defendant to take reasonable measures to protect Plaintiff's and the Class's sensitive data and is a further source of Defendant's duty to Plaintiff and Class Members. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to use reasonable measures to protect highly sensitive data. Defendant, therefore, was required and obligated to take reasonable measures to protect data it possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect sensitive information. By failing to implement reasonable data security measures, Defendant acted in violation of § 5 of the FTC Act.

137. Defendant is obligated to perform its business operations in accordance with Federal, State as well as industry-specific standards. Industry standards are another source of duty and obligations requiring Defendant to exercise reasonable care with respect to Plaintiff and Class

Members by implementing reasonable data security measures that do not create a foreseeable risk of harm to Plaintiff and Class Members.

138. Defendant breached its duty to Plaintiff and Class Members by implementing unreasonable data security measures and by failing to keep data security "top-of-mind" despite understanding and writing about the risk of data breaches involving highly sensitive data and touting its own security capabilities.

139. Defendant was fully capable of preventing the Data Breach. Defendant, as a sophisticated and experienced technology company, knew of data security measures required or recommended by the FTC, state laws and guidelines, and other data security experts which, if implemented, would have prevented the Data Breach from occurring at all, or limited the scope and depth of the Data Breach. Defendant thus failed to take reasonable measures to secure its system, creating vulnerability to a breach.

140. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer injury, including the ongoing risk that their data will be used nefariously against them or for fraudulent purposes.

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

141. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs.

142. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

143. Change Healthcare is a HIPAA covered business associate that provides services to various healthcare providers (*i.e.*, HIPAA "Covered Entities"). As a regular and necessary part

of its business, Change Healthcare collects and stores the highly sensitive PHI of its clients' patients. Change Healthcare has a duty under federal law to maintain the strictest confidentiality of the patients' PHI that it acquires, receives, and collects, and Change Healthcare is further required to maintain sufficient safeguards to protect that PHI from being accessed by unauthorized third parties.

144. Defendant violated HIPAA and Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of this Data Breach.

145. Defendant's violation of HIPAA and Section 5 of the FTC Act constitute negligence *per se*.

146. Plaintiff and Class Members are consumers within the class of persons HIPAA and Section 5 of the FTC Act were intended to protect.

147. Moreover, the harm that has occurred is the type of harm that HIPAA and the FTC Act were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

148. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class)

149. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs.

150. Acting in the ordinary course of business, Defendant contracts with several healthcare providers to facilitate services being provided to patients. Defendant obtains patients' PHI as part of its ordinary course of business to perform its business functions.

151. Upon information and belief, each of those respective contracts contained provisions requiring Defendant to protect the patient information that it received in order to provide such functions in carrying out the business of the contract.

152. Upon information and belief, these provisions requiring Defendant acting in the ordinary course of business to protect the personal information of patients were intentionally included for the direct benefit of Plaintiff and class members, such that Plaintiff and class members are intended third party beneficiaries of these contracts, and therefore entitled to enforce them.

153. Defendant breached these contracts while acting in the ordinary course of business by not protecting Plaintiff's and class member's personal information, as stated herein.

154. As a direct and proximate result of the breaches described in detail herein, Plaintiff and class members sustained actual losses and damages. Plaintiff and class members alternatively seek an award of nominal damages.

FOURTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

155. Plaintiff repeats and re-alleges the allegations set forth in the preceding paragraphs.

156. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those

alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

157. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to safeguarding the data of Plaintiff and the Class. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of additional fraud against them or on their accounts.

158. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to secure the sensitive information with which it is entrusted, and to notify impacted individuals of the Data Breach under the common law, HIPAA, and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its legal duty by failing to employ reasonable measures to secure customers' personal and financial information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

159. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect their clients' (*i.e.*, Plaintiff's and the Class's) data.

160. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data system. If another breach of Defendant's data system occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

161. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

162. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for relief as follows:

a. For an Order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, and appointing Plaintiff and her Counsel to represent the Class;

b. For an Order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. Declaratory and injunctive relief as described herein;

e. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

f. Awarding pre- and post-judgment interest on any amounts awarded; and

g. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: March 22, 2024

Respectfully submitted,

/s/ J. Gerard Stranch, IV
J. Gerard Stranch, IV, BPR 23045
Michael Iadevaia, BPR 041622
Emily Schiller, BPR 039387
STRANCH, JENNINGS & GARVEY PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Telephone: (615) 254-8801
gstranch@stranchlaw.com
miadevaia@stranchlaw.com
eschiller@stranchlaw.com

LEEDS BROWN LAW, P.C.
Jeffrey K. Brown *
Brett R. Cohen *
jbrown@leedsbrownlaw.com
bcohen@leedsbrownlaw.com
One Old Country Road, Suite 347
Carle Place, NY 11514-1851
Tel: (516) 873-9550

LEVIN SEDRAN & BERMAN LLP
Charles E. Schaffer *
cschaffer@lfsblaw.com
510 Walnut St., Ste 500
Philadelphia, PA 19106
Tel: (215) 592-1500

GOLDENBERG SCHNEIDER, LPA
Jeffrey S. Goldenberg *

Todd B. Naylor *
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com
4445 Lake Forest Dr., Ste. 490
Cincinnati, OH 45242
Tel: (513) 345-8291

Counsel for Plaintiff & the Putative Class

Pro hac vice forthcoming *